(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 723 216 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
20.06.2001 Bulletin 2001/25

(51) Int Cl.7: **G06F 1/00**, G11B 20/00

(21) Application number: **95118162.7**

(22) Date of filing: **17.11.1995**

(54) Compact disc player security system reproducing method and apparatus

Wiedergabeverfahren und Einrichtung von Kompaktplatten und Kompaktplattenspieler-Sicherheitssystem

Procédé et dispositif de reproduction de disques compacts et système de sécurité de lecteur de tels disques

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB IT LI NL SE

(30) Priority: **18.11.1994 JP 28539094**

(43) Date of publication of application:
24.07.1996 Bulletin 1996/30

(60) Divisional application:
01108855.6

(73) Proprietor: **Sony Computer Entertainment Inc.**
Tokyo 107-0052 (JP)

(72) Inventors:
- **Kutaragi, Ken, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)
- **Hirano, Tetsuya, c/o Sony Corporation**
  Shinagawa-ku, Tokyo (JP)

(74) Representative: **Müller, Frithjof E., Dipl.-Ing. et al**
Patentanwälte
MÜLLER & HOFFMANN,
Innere Wiener Strasse 17
81667 München (DE)

(56) References cited:
EP-A- 0 325 330
EP-A- 0 545 472
EP-A- 0 553 545
EP-A- 0 637 023

EP 0 723 216 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates to a digital storage medium which has in a track of a plurality of data bits a security code which is defined by modulating an offset of the physical position of the data bits from a nominal track position, a method of preventing a computer software operated system from operating with unauthorized software contained in a digital storage medium, an apparatus for reading a security code stored in a digital storage medium, a method of storing a security code on a digital storage medium, and an apparatus for carrying out said storing method in accordance with the precharacterizing parts of the independent claims 1, 9, 15, 19, and 23, respectively.

Description of the Related Art

[0002] Recently in the field of data storage and retrieval, the use of optical compact discs has grown significantly. Digital optical storage devices have the advantage of having a large storage capacity compared with other forms of data storage. In these systems, it is often desirable to protect a dedicated player system from being used with unauthorized software. This is especially true in the video game market where video game manufacturers typically sell game playing devices at or near their cost with the expectation that sales and royalties on the software for the games will provide a large return.

[0003] Conventional systems for protecting devices which are capable of operating with a variety of computer software typically employ a security code to protect the system from being used with unauthorized computer software. In a conventional system for preventing a dedicated disc reproducing apparatus from being used with unauthorized software, the system initially determines whether a security code is present at a predetermined memory location of the storage medium which contains the software. The player or reproducing apparatus determines whether or not the software is authorized by comparing the data stored in the predetermined memory location with a security code. This is generally known as a security system or protect processing.

[0004] In recent years, there has been a number of instances where even systems which have protect processing or security systems have been subject to use with unauthorized computer software. There have been instances where the protect processing has been illegally avoided even with the security system as described above. One reason for this is that in conventional security systems the security code is located in a predetermined memory location which can be readily identified by examining the software. This is also at least partially due to the fact that the determination as to whether or not this recording medium is authorized and execution of the computer program are carried out by the same hardware. The present invention addresses these problems and overcomes the shortcomings of the prior art.

[0005] EP-A-0 545472 describes a closed information system with physical copy protection in accordance with the precharacterizing parts of the independent claims 1, 9, 15, 19, and 23, respectively. The digital storage medium disclosed therein stores information in form of variations of a first physical parameter, e. g. in form of modulated pits. Further the digital storage medium exhibits a second variation of a second physical parameter which differs from the first physical parameter defining the information, but which is of a type that is detectable by means of the transducer of the playback apparatus. In one embodiment of the known digital storage medium, the variation of the second physical parameter is a variation of the track position in a direction transverse to the track direction, i. e. in form of a radial track wobble. Further, this document describes that instead of a radial wobble with a constant frequency and constant amplitude radial wobbles can be used which exhibit a modulation which represents a code. Such modulation may be an FM-modulation.

[0006] EP-A-0 553 545 describes a CD ROM disc and security check method for the same. A security code is recorded in a predetermined code region in a sector of a boot sector in the innermost track of the CD ROM disc. The security code indicates that the CD ROM disc is duly licensed, namely by a television game machine producer. The security code further may contain a program to be executed after a checking operation of the security code. This document does not disclose a special modulation scheme for the recording of the security code.

[0007] EP-A-0 325 330 describes a known digital storage medium which provides a sinusoidal radial track wobble which frequency is modulated with a position information signal. When an information signal is recorded on the digital storage medium which is of an inscribable type, the position information signal is recovered by means of the variations in the scanning beam produced by the track wobble modulation.

SUMMARY OF THE INVENTION

[0008] The present invention provides a digital optical compact disc recording medium which incorporates an improved system for storing and accessing the security code to prevent copying of computer software from an unauthorized disc onto a dedicated disc player. In order to solve the above-mentioned problems, a digital storage medium (a disc) comprises a first side and a second side, a plurality of data bits stored in a track on the first side, and a security code stored in the track, said security code being defined as a modulation of a positional offset of the physical location of the data bits from a nominal track location is characterized in that the modulation of the positional offset of the physical location is a binary modulation, wherein an offset of the data bits is defined

as a first logic state and a lack of offset from a nominal track location is defined as a second logic state.

[0009] Further, in order to solve the above mentioned problems, a method of preventing a computer software operated system from operating with unauthorized software contained in a digital storage medium (a disc) having a plurality of data bits stored on a side of said storage medium in form of a track of said data bits, wherein a security code is stored in the track of said storage medium, said security code being defined as a modulation of a positional offset of the physical location of the data bits from a nominal track location, is characterized by comprising the steps of (a) examining a track of data bits on the digital storage medium for the binary offset modulation of the data bits wherein an offset of the data bits from the nominal track location is defined as a first logic state and a lack of offset of the data bits from the nominal track location is defined as a second logic state, (b) demodulating the binary offset modulation to define a digital code which represents said security code, (c) comparing the digital code with a predetermined security code to determine, if the demodulated digital code matches the predetermined security code, (d) accepting the digital storage medium as authentic and passing control of the software operated system to the computer software stored in the digital storage medium, if the digital code matches the predetermined security code, and (e) rejecting the digital storage medium, if the digital code does not match the predetermined security code.

[0010] The security verification method according to the present invention comprises the steps of reading out the modulated physical offset or wobbling of the data bits in the radial direction of the recording medium so that the security code can be detected. The detection step of detecting the certification data or security code is followed by a discrimination step of determining whether or not the certification data which is detected corresponds to a security code previously set in advance. It should be noted that when it is determined during the discrimination step that certification data and the security code set in advance do not match each other, the system inhibits further processing of the disc software, thus preventing unauthorized software from being used with the system.

[0011] Additionally, the above-mentioned disc recording and reproducing method includes the step of displaying video information identifying the game manufacturer as the licenser or creator of the software. This occurs only when the certification data corresponds with or matches the security code. In the preferred embodiment of the present invention, this occurs after a second check or verification which ensures that the disc contains a proprietary video image or message at predetermined locations of the disc. By incorporating this step into the process of reading the software from the disc, the game manufacturer is able to force anyone who makes unauthorized software for use with the system to violate the copyright or trademark laws. This occurs because the system will automatically display a proprietary screen identifying the game station manufacturer as the creator or licenser of the software. If the software is unauthorized, its creator will automatically be in violation of the trademark laws because the software is not actually authorized or licensed as stated by the display screen.

[0012] In order to solve the problems mentioned above, the present invention provides an apparatus for reading a security code stored in a digital storage medium (a disc) comprising a first side and a second side and a plurality of data bits stored on the first side of said digital storage medium in the form of a track of data bits, and a security code stored in the track said security code being defined as a modulation of a positional offset of a physical location of the data bits from a nominal track location, wherein said apparatus comprises a means for reading the physical offset modulation from the nominal track position of a plurality of data bits stored on said digital storage medium, said apparatus being characterized in that it comprises further a detector means for detecting a code which is defined as a binary modulation of said physical positional offset so that an offset of the data bits is defined as a first logic state and a lack of offset from the nominal track location is defined as a second logic state, said detector means having an input connected to the output of the reading means, a discriminator means for determining whether the code detected by the detector means matches a predetermined security code stored in a memory associated with the apparatus, and a controller for controlling reproduction of data stored in the digital storage medium depending on an output from the discriminator means.

[0013] The physical position of the bits is modulated in the radial direction to define a security code. The security code therefore does not reside in a predetermined memory location but rather is embedded in a general area of the disc by modulating the location of the data bits with respect to a nominal track position. This is advantageous because a person examining the software would be unable to determine the security code. In the preferred embodiment, the presence of the physical offset or modulating is defined to be a logical "1" and the absence of wobbling is defined to be logical "O".

[0014] A detecting means for detecting certification data which has been stored by modulating the physical position of a plurality of data bits determines the security code. In a preferred embodiment, the optical read head is divided in two parts in order to determine whether the security code is present. Data bits which are offset from a nominal track location can be detected with such a device. The main data comprising the software for the computer game stored on the disc is also read out with the same read head.

[0015] In the preferred embodiment of the present invention, the system performs an initial check to determine whether or not the disc contains a "wobbled" code in the TOC (Table of Contents) area of the disc. In an

authorized disc, the security code is repeated several times in order to ensure that it is properly detected without the need to add error correction bits to the security code. The system initially checks to determine whether the disc contains wobbling of the data in the TOC area of the disc before actually checking the actual code. If the disc does not contain a wobbled code, the system then determines, if the disc is actually an audio disc. if it is an audio disc, the system proceeds to play the audio disc and provide an audio output. If it is not an audio disc, then the system shuts down.

[0016] If the disc does contain a "wobbled" code in the TOC area of the disc, the player proceeds to decode the wobbled code and transmit this decoded data to a mechanical controller. If the wobbled code matches a predetermined security code, then the system performs a second check on the disc for verifying authenticity. If the wobbled code does not match, the player then checks to see, if the disc is an audio disc as noted above. If the disc passes the first code verification, the disc player then proceeds to verify that the disc contains a logo which matches a logo stored in the system. This second verification is performed to verify that the disc is actually authorized.

[0017] According to a further aspect of the present invention, a method of storing a security code on a digital storage medium (a disc) comprises following steps: (a) generating a digital security code, (b) moving the digital storage medium with respect to a laser source, (c) positioning the laser source over an unrecorded track location of the digital storage medium, and is characterized by the steps of: (e) recording a plurality of digital data bits on the digital storage medium by binary modulating an offset of a position of the laser beam on the disc from a nominal track position to define a logical condition of a data bit of the security code, wherein an offset of the data bit is defined as a first logic state and lack of offset from a nominal track location is defined as a second logic state.

[0018] A preferred embodiment of the disc player security system of the present invention is described in detail below with reference to the attached drawings. Although the preferred embodiment is described with reference to a video game player system it is recognized that this is exemplary only.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019]

FIG. 1 illustrates a block diagram of an exemplary embodiment of the security system of the present invention;

FIG. 2A illustrates the typical physical relationship of data bits stored in a track on a digital optical disc;

FIG. 2B illustrates the physical offset modulation or wobbling or the data bits from a nominal track position according to the present invention;

FIG. 3 illustrates decoding of the modulated output based on a physical "wobbling" of the data bits which defines digital data.

FIG. 4 illustrates a block diagram of an exemplary optical decoder for use with the present invention;

FIG. 5 illustrates a flow chart explaining operation of the disc player security system of the present invention;

FIG. 6 illustrates an exemplary video display output which is to be displayed after it is determined that the disc has proprietary logo information stored in predetermined memory locations; and

FIG. 7 illustrates a system for encoding a security code on a ditial optical disc through offsetting the physical position of a plurality of data bits from a nominal track position in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] A preferred embodiment of the disc reproducing apparatus according to the present invention is set forth below with reference to the drawings. In this preferred embodiment, a video game device employs the security system to prevent unauthorized use of a machine with software contained on a digital compact disc. A digital optical compact disc which embodies the present invention has its main or primary data recorded in a conventional manner via EFM (Eight to Fourteen modulation) in NRZ (Non Return to Zero) format. This information resides in the normal track and sector locations on the disc. This is similar to the manner in which conventional audio compact discs are encoded. In the preferred embodiment of the present invention, the data bits which define the TOC (Table of Contents) area of the disc are stored such that a wobbled security code is embedded In the TOC track as a modulation of a physical positional offset from a nominal track location. The security code is stored by a process in which a 22.05 kHz signal is used as the modulation carrier wave which is digitally modulated in NRZ (Non Return to Zero) format to encode the security code. The positional offset which defines the security code Is a physical offset in the radial direction of the optical disc. The frequency of the offset is based on the linear velocity of the optical head passing over the track and the resultant reproduction of the offset as an RF signal. It should be noted that the 22.05 kHz signal is a signal having a frequency which is one-half of the sampling frequency of the digital optical compact disc. (44.1 kHz) This allows accurate

reproduction of the offset or wobbling signal. The TOC portion of the disc thus has two forms of information stored in this area. First, the TOC may have information digitally encoded and defined as the pits and holes that make up the TOC track. Additionally, the security code is stored through a modulation of a positional offset of the data bits from a nominal track position.

[0021] The security code which is stored in the TOC area of a digital optical compact disc in accordance with the present invention thus does not reside in a specific or predetermined track and sector location on the digital optical compact disc. The security code data is typically only several bytes in length. In the preferred embodiment of the present invention, because the security code is not stored in a specific addressable location, it Is more difficult for a person examining the software to copy the security code. The code is repeatedly encoded in the TOC area of the disc so that the optical pick-up 2 and security code detector are more likely to correctly identify the presence of the security code.

[0022] FIG. 1 illustrates a block diagram of the system used for decoding a security code in accordance with the present Invention. In this illustration an optical pick up 2 generates a signal by reading the positional fluctuation of data bits on the disc 1 in the radial direction with respect to a nominal track position. This is considered to be "wobbled" data. Although a single pick-up head generates both the security code and the primary data stored on the disc, two separate hardware sections in the game player process these signals.

[0023] A security code detecting section 3 detects the presence of security code based on the so-called "wobbled" data.' A disc reproduction control section 4 correlates the security code with a predetermined code stored in the system's memory to determine whether or not the disc is an authorized disc. A main data demodulation section 5 reads out the primary or main data stored on the compact disc for use with the disc player machine. This main data is either the software for a video game or it may alternatively be audio information defining a sound recording. The main data demodulating section 5 feeds a main data buffer 6 having an output which in turn also feeds an interface section 7. The program execution control section 8 controls execution of the software contained on the disc. Display of video information is produced by the display 10. The display is controlled by the display control section 11. The display 10 displays the game information after successful completion of the security code verification. In the preferred embodiment of the present invention, the system also performs a second check to verify that the disc is authentic. This second check verifies that a logo stored in a predetermined location on the compact disc matches a logo stored on the machine. If an audio disc has been inserted into the player, the system will provide an audio signal output from terminal 9.

[0024] Figure 2 A Is a greatly enlarged view which illustrates data bits stored on a typical conventional digital optical disc, For the sake of illustration, the data bits are shown in a linear arrangement, however, those skilled in the art will appreciate that the data bits are actually arranged on a conventional disc in a slightly curved pattern to match the curvature of the tracks on the disk. This is also true of digital optical discs which embody the present invention. Figure 2 8 illustrates the presence of a wobbled code wherein the physical position of the Information bits on the disc are modulated as an offset *from a* nominal track position to provide a modulated signal which, in the preferred embodiment, is a security code for the disc. The positional offset of the data bits from a nominal track location is in the radial direction of the recording medium. In the preferred embodiment of the present invention the security code is located in the Table of Contents (TOC) area of the disc, however, it is contemplated that other track locations on the disc are equally suitable.

[0025] Because the security code is stored numerous times in the TOC area of the disc, the security code can be more reliably reproduced without the need for storing additional error correction bits. The disc player Is thus more likely to reproduce the security code accurately if there Is a scratch or dust on the disc. Storing the security code numerous times in the TOC area of the disc allows the security code to be stored without also storing additional error correction bits.

[0026] Figure 3 illustrates an example of the resultant digital output from the security code detecting section wherein the presence of wobbling or the physical offset of the data bits ed:15-12-2000 minal track position indicates a logical "1" and the lack of wobbling or lack of offset from a nominal track position is Indicated as a logical "0". In the preferred embodiment the security code is stored in NRZ (Non return to zero) format. It is understood, however, that alternate schemes for encoding the security code are also possible. In the preferred embodiment the frequency of the offset for the security code is 22.05 kHz which is one half of the sampling frequency of conventional optical compact discs. As seen in the illustration of Figure 3, the security code is digitally encoded through the presence and absence of a physical offset of the data bits which, when present, is at a frequency of 22.05 kHz. The security code is repeatedly stored in the TOC area of the disc several times as noted.

[0027] Figure 4 illustrates an optical signal decoder and corresponding decoding hardware for use with the present invention. The optical detector 13 is comprised of a two part photodetector which is divided into two halves that are positioned above a nominal track position on the disc. The two part photodetector 13 provides one pair of output signals. The pair of output signals is applied to two corresponding inputs of a differential amplifier 15. The differential amplifier has its output connected to the input of a low pass filter 17 which has its output connected to the input of the tracking server 18. The tracking server 18 performs positional control of the

optical detector 13.

[0028] The output of the differential amplifier 15 which is considered to be an RF signal also feeds an input of a 22.05 kHz band pass filter 20. The output of the 22.05 kHz band pass filter 20 feeds the input of a peak hold circuit 21. The output of the peak hold is applied to the input of a comparator 22. The peak hold circuit 21 provides a digital output comprising the signal decoded by examining the TOC track for the presence of "wobbling" or the offset of the data bits from a nominal track position. Because the photodetector 13 is divided into two separate areas, the difference of the two signals generated by the two photodetector areas, identifies the presence of a wobbling or security code which in the preferred embodiment has a frequency of 22.05 kHz. As shown in Figures.2 and 3, it d:15-12-2000 actual physical offset of a single data bit which defines a particular bit of the security code, but rather each bit of the security code is defined as the presence or absence of wobbling over a brief period of time. The comparator 22 makes a determination as to whether the disc is authentic based on whether the security code matches a code previously stored in the memory of the disc player. The output of the comparator 22 feeds the Input of the disc controller 24.

[0029] The pair of outputs from the two pair photodetector 13 also feeds the two inputs of an adder 26. The adder 26 provides a digital output which consists of the main or primary data stored on the disc. This Is the data which is determined by the pits and holes on the disc. An output from the adder 26 feeds an amplifier 27 which has an output which is connected to an Input of a signal processor 30 for processing the primary data stored on the disc.

[0030] A flow chart for explaining the operation of a preferred embodiment of the disc reproducing apparatus is shown in FIG. 5. The security code detecting section 3 of Figure 1 initially determines whether a 22.05 kHz signal is present as an RF signal generated by the optical pick-up head. This is based on the output from the optical detector 13. If there is wobbling of the data on the disc, the optical detector 13 will provide an RF signal which corresponds to the frequency of the positional offset of the data bits from a nominal track position. In the preferred embodiment of the present invention this is a 22.05 kHz signal. This step is identified as step S1 in the flow diagram of Figure 5. If it is determined such an RF signal exists as an output from the optical detector, then in step S2, it is determined whether or not the 22.05 kHz signal is in an a.c. state. The determination of whether the 22.05 kHz signal is in an a.c. state is not a determination of whether there is a periodic waveform, but rather this is a determination of whether the wobbled signal changes logical states frequently as identified in Figure 3. This first check will exclude discs from use on the machine which do have wobbling of the data bits in the TOC track but which do not have the wobbled track modulated to define a digital signal.

[0031] If it is determined that the 22.05 kHz signal is in an a.c. state, predetermined demodulation processing in which the 22.05 kHz signal is considered the carrier is performed on the RF signal generated by the optical pick-up in step S3. This is the detection of the security code with the system set forth in Figure 4. The security code stored on the disc Is thereby determined. The security code is then sent to the reproduction control section 4 as shown in Figure 1. Also If it is determined that the optical pick-up has not generated a 22.05 kHz signal or if it is determined to be in a d.c. state (no wobbling or offset), a signal indicating that the a.c. signal does not exist is sent to the reproduction control section 4.

[0032] The disc reproduction control section 4 determines whether the security code stored on the disc and the security code stored on the game or disc reproduction device match or correspond with each other. This occurs in step S4. This determines whether the disc is an authorized disc for the system.

[0033] In the system of the present invention, If the disc passes the security code matching which compares the security code stored on the player machine with the wobbled code stored on the disc, the system then performs a second verification. In step S5, the system reads out a logo and/or license data from the disc in order to perform the second verification. The second verification is performed in step S6 wherein the system compares a logo and/or license data stored in memory of the machine with the contents of predetermined memory or storage locations on the disc. This second verification also determines whether the disc is authentic.

[0034] Step S7 of Figure 5 is a step wherein the system will display a visual image identifying the software as being produced or licensed by the game manufacturer. This would force someone who illegally copies the security code to violate the trademark laws because the system would identify the software as being licensed when it is actually not licensed. in the preferred embodiment of the present invention, a logo stored in a memory associated with the player machine is compared with a logo stored in a predetermined memory location on the disc. This occurs in step S6. The system passes control to the software contained on the disc only if the two logos or images match. The system ceases operation if the two logos do not match. This second verification is performed to increase the likelihood of eliminating unauthorized discs from use on the machine. if there is a match, the system will then display the proprietary visual image in step S7. This is described further below.

[0035] If it is determined through the two verifications that the disc is authentic, a control signal is generated to instruct that main data transfer occur and that control be passed to the software stored on the disc. The program execution control section 8 illustrated in Figure 1 sends a signal to the interface section 7 so that the software stored on the disc can be transferred onto the system memory In order to transfer control to this software.

This occurs in step S8 of the flow diagram illustrated in Figure 5. Step S8 which is execution of the disc content will not occur unless the disc also passes the second verification of step S6.

[0036] On the other hand, if the security code does not match, or if the 22.05 kHz signal does not exist or if the 22.05 kHz signal is not in an A.C. state, or if the logo does not match the logo on the disc, it is then determined whether the disc is merely an audio disc. This is step S9 in the flow diagram of Figure 5. If the disc is an audio disc, the system will allow the disc to be played on the unit because it is more desirable that a game device have this alternate capability. The system then outputs an audio signal as identified in step S10 of the flow diagram of Figure 5. Alternatively, in step S11, if it is determined that the disc is not an audio disc, the system will stop reproduction of the data from the disc and control will not pass to the software on the disc.

[0037] Figure 6 illustrates an exemplary proprietary display which may be used to eliminate disc counterfeiters. The display may include one or more of the visual indicators identified on the screen 50. A registered trademark 51 may be used to force a counterfeiter to violate the trademark laws. Alternatively, an image identifying the software as being licensed by the machine manufacturer may also be used as indicated by block 52. A company name may also be used as indicated by block 53. All of these additional items may be used together or only-select ones may be used. These visual indications can be stored in a memory of the system and compared with the contents of specific memory locations on the disc in accordance with the second check or verification identified above. This second verification is identified as step S6 in the flow diagram of Figure 5. Alternately, a simple code matching may be used to further verify that the disc is authorized. For example, an ASCII code stored in a memory associated with the machine may be compared with the contents of predetermined storage locations on the disc.

[0038] FiG. 7 illustrates a system for encoding the wobbled security code of the present invention on a digital optical compact disc. Pre-Mastered CD 31 (PMCD) is a master disc having a game program, game data and identification data which identifies the type of the disc stored thereon. The identification data is recorded in a predetermined area of the master disc. The identification data indicates whether the master disc is to be used with a particular game playing device and identification of which country or area of the game is to be used. For example, this information could be Game X - Master Disc - "Japan". The pick-up 33 reads the digitally encoded information from the master disc 31. The detector 34 detects the Identification data and the controller 25 transfers the identification to the security code generator 37 if the master disc is identified as being authentic. If the identification data is not detected, the cutting machine operates only as a conventional cutting machine for a compact disc and will not insert a wobbled code.

[0039] The security code generator 37 generates a binary security code which depends on the particular country in which the disc is to be sold. For example, the following codes could be used:

Master Disc - Japan = ABCD
Master Disc - USA = EFGH
Master Disc - Europe = WXYZ

[0040] The AOD (Acoustic Optic Deflection circuit) drive amplifier 38 amplifies a signal generated by the security code generator 37. The AOD deflection circuit 39 receives an output from the AOD drive amplifier and outputs an RF signal which modulates the physical position of the laser beam with respect to a nominal track position depending on the security code which is supplied from the security code generator 37 in accordance with the coding scheme identified above. For example, the presence of an offset may indicate a logical "1" or first logical condition and the absence of wobbling may indicate a logical "0" or second logical state. The AOD drive 39 is the element which moves the laser in the radial direction off of a nominal track position location for encoding the pits on the CD. The pits on the CD are thus wobbled in response to the RF signal output from the AOD drive amp 39. The physical placement of the pits on the disc is thus modulated from a nominal track position in order to define the security code. The EFM unit 40 encodes the game program and game data as a 14-bit word based on an original 8 bit word. This is known as Eight-to-Fourteen Modulation (EFM). The recording laser 42 provides a signal which cuts the pits on the master disc 45 in a conventional manner after reflection by a mirror 43 and passing through a lens 44. The signal output from the laser 42 is positionally controlled via the AOD 39.

Claims

1. A digital storage medium (1) comprising a first side and a second side;

   a plurality of data bits stored in a track on the first side: and
   a security code stored in the track, said security code being defined as a modulation of a positional offset of the physical location of the data bits from a nominal track location.

   characterized in that
   the modulation of the positional offset of the physical location is a binary modulation, wherein an offset of the data bits is defined as a first logic state and a lack of offset from a nominal track location is defined as a second logic state.

2. The digital storage medium according to claim 1,

wherein the positional offset of the data bits has a wobble frequency of 22.05 kHz.

3. The digital storage medium of claim 1, wherein the modulation of the positional offset of the physical location of the data bits is in radial direction of the recording medium.

4. The digital storage medium of claim 1, wherein the first logic state is a logical "1".

5. The digital storage medium of claim 1, wherein the security code is stored in a non-return to zero format.

6. The digital storage medium of claim 1, wherein said digital storage medium is a digital optical compact disc, and the security code is stored in the TOC area therein.

7. The digital storage medium of claim 6, wherein the security code is repeatedly stored in the TOC area of the compact disc.

8. The digital storage medium of one of the preceding claims, wherein said security code has a given number of bits, each of which is represented by one of said first and second logic states.

9. A method of preventing a computer software operated system from operating with unauthorized software contained in a digital storage medium having a plurality of data bits stored on a side of said storage medium in form of a track of said data bits, wherein a security code is stored in the track of said storage medium, said security code being defined as a modulation of a positional offset of the physical location of the data bits from a nominal track location,

said method being **characterized by** comprising the steps of:

(a) examining a track of data bits on the digital storage medium for a binary offset modulation of the data bits, wherein an offset of the data bits from the nominal track location is defined as a first logic state and a lack of offset of the data bits from the nominal track location is defined as a second logic state;
(b) demodulating the binary offset modulation to define a digital code which represents said security code;
(c) comparing the digital code with a predetermined security code to determine, if the demodulated digital code matches the predetermined security code;
(d) accepting the digital storage medium as authentic and passing control of the software operated system to the computer software stored in the digital storage medium, if the digital code matches the predetermined security code; and
(e) rejecting the digital storage medium, if the digital code does not match the predetermined security code.

10. The method according to claim 9, wherein said security code has a given number of bits, each of which is represented by one of said first and second logic states.

11. The method according to claims 9 or 10, further comprising an additional step of displaying a predetermined video image only when the step of comparing the digital code with a predetermined security code determines that the digital code matches the predetermined security code.

12. The method according to claims 9 or 10, further comprising an additional step of operating the system in accordance with software stored in the digital storage medium only, when the step of comparing the digital code with the predetermined security code determines that the digital code matches the predetermined security code.

13. The method according to claims 9 or 10, further comprising an additional step of performing a second verification, wherein the system compares a further code stored in a memory associated with the system with a code stored under a predetermined address in the digital storage medium, and a step of rejecting the digital storage medium, if the further code does not match the code stored under the predetermined address in the digital storage medium.

14. The method according to claim 13, wherein the further code is a proprietary logo and the method comprises the additional step of displaying the logo on a display screen associated with the system, if the further code matches the code stored under the predetermined address in the digital storage medium.

15. An apparatus for reading a security code stored in a digital storage medium comprising a first side and a second side and a plurality of data bits stored on the first side of said digital storage medium in the form of a track of data bits, and a security code stored in the track, said security code being defined as a modulation of a positional offset of a physical location of the data bits from a nominal track location, wherein said apparatus comprises:

a means for reading the physical offset modulation from the nominal track position of a plurality of data bits stored on said digital storage medium,

characterized in that the apparatus further comprises:

a detector means (3: 20) for detecting a code which is defined as a binary modulation of said physical positional offset so that an offset of the data bits is defined as a first logic state and a lack of offset from the nominal track location is defined as a second logic state, said detector means having an input connected to the output of the reading means;
a discriminator means (22) for determining whether the code detected by the detector means (3; 20) matches a predetermined security code stored in a memory associated with the apparatus; and
a controller (24) for controlling reproduction of data stored in the digital storage medium depending on an output from the discriminator means (22).

16. The apparatus according to claim 15, wherein said security code has a given number of bits, each of which is represented by one of said first and second logic states.

17. The apparatus according to claims 15 or 16, further comprising:

means for reading data stored in a plurality of data bit locations under a predetermined address in the digital storage medium, said reading means having an output;
means for detecting a second code stored in said plurality of data bit locations under said predetermined address, said detecting means being connected to the output of the reading means; and
a second discriminator means for determining whether the second code matches a further predetermined code stored in a memory associated with the apparatus.

18. The apparatus according to claim 17, wherein the second code defines a logo and wherein the apparatus further comprises means for displaying the logo, if it is determined that the second code matches the further predetermined code.

19. A method of storing a security code on a disc-like digital storage medium comprising the following steps:

(a) generating a digital security code;
(b) moving the digital storage medium with respect to a laser source (42);
(c) positioning the laser source (42) over an unrecorded track location of the digital storage medium (45);

characterized by the steps of:

(e) recording a plurality of digital data bits on the digital storage medium (45) by binary modulating an offset of a position of the laser beam on the digital storage medium from a nominal track position to define a logical condition of a data bit of the security code, wherein an offset of the data bits from the nominal track position is defined as a first logic state and lack of offset from the nominal track position is defined as a second logic state.

20. The method according to claim 19, wherein the first logic state is a logical "1".

21. The method according to claim 19, wherein the step of offsetting the laser beam from the nominal track position provides a positional offset wobble of the track position having a wobbling frequency of substantially equal to 22.05 kHz.

22. The method according to one of the claims 19 to 21, wherein said security code has a given number of bits, each of which is represented by one of said first and second logic states.

23. An apparatus carrying out the method of one of the claims 19 to 22,
characterized in that said apparatus comprises:

a security code generator (37) for providing the digital security code;
an output of the security code generator (37) being connected to an input of an acoustic optical deflection amplifier (38);
an output from the acoustic optical deflection amplifier (38) being connected to a first input of an acoustic optical deflection circuit (39); and
a recording laser (42) having an output connected to a second input of the acoustic optical deflection circuit (39).

Patentansprüche

1. Digitales Speichermedium (1) mit:

- einer ersten und einer zweiten Seite;
- einer Anzahl von in einer Spur auf der ersten Seite gespeicherten Datenbits und
- einem in der Spur gespeicherten Sicherheitscode, der als Modulation eines Positionsversatzes des körperlichen Orts der Datenbits gegenüber einem Nenn-Spurort definiert ist;

dadurch gekennzeichnet, dass

- die Modulation des Positionsversatzes des körperlichen Orts eine Binärmodulation ist, wobei ein Versatz der Datenbits als erster logischer

Zustand definiert ist und ein fehlender Versatz gegenüber einem Nenn-Spurort als zweiter logischer Zustand definiert ist.

2. Digitales Speichermedium nach Anspruch 1, bei dem der Positionsversatz der Datenbits eine Wobbelfrequenz von 22,05 kHz aufweist.

3. Digitales Speichermedium nach Anspruch 1, bei dem die Modulation des Positionsversatzes des körperlichen Orts der Datenbits in radialer Richtung des Aufzeichnungsmediums vorliegt.

4. Digitales Speichermedium nach Anspruch 1, bei dem der erste logische Zustand dem logischen Wert "1" entspricht.

5. Digitales Speichermedium nach Anspruch 1, bei dem der Sicherheitscode in einem NRZ(Non-Return to zero)-Format gespeichert ist.

6. Digitales Speichermedium nach Anspruch 1, das eine digitale optische CD ist und der Sicherheitscode in deren TOC-Bereich gespeichert ist.

7. Digitales Speichermedium nach Anspruch 6, bei dem der Sicherheitscode wiederholt im TOC-Bereich der CD gespeichert ist.

8. Digitales Speichermedium nach einem der vorstehenden Ansprüche, bei dem der Sicherheitscode über eine vorgegebene Anzahl von Bits verfügt, von denen jedes durch den ersten oder zweiten logischen Zustand repräsentiert ist.

9. Verfahren zum Verhindern des Betriebs eines durch Computersoftware betriebenen Systems durch unberechtigte Software auf einem digitalen Speichermedium mit einer Anzahl von auf einer Seite des Speichermediums in Form einer Spur von Datenbits gespeicherten Datenbits, wobei in der Spur des Speichermediums ein Sicherheitscode gespeichert ist, der als Modulation eines Positionsversatzes des körperlichen Orts der Datenbits gegenüber einem Nenn-Spurort definiert ist;

- wobei das Verfahren **dadurch gekennzeichnet** ist, dass es die folgenden Schritte aufweist:

(a) Untersuchen einer Spur von Datenbits auf dem digitalen Speichermedium nach einer Binärversatz-Modulation der Datenbits, wobei ein Versatz der Datenbits gegenüber dem Nenn-Spurort als erster logischer Zustand definiert ist und fehlender Versatz der Datenbits gegenüber dem Nenn-Spurort als zweiter logischer Zustand definiert ist;

(b) Demodulieren der Binärversatz-Modulation zum Definieren eines den Sicherheitscode repräsentierenden digitalen Codes;

(c) Vergleichen des digitalen Codes mit einem vorbestimmten Sicherheitscode zum Ermitteln, ob der demodulierte digitale Code mit dem vorbestimmten Sicherheitscode übereinstimmt;

(d) Akzeptieren des digitalen Speichermediums als echt und Übergeben der Steuerung des Software-betriebenen Systems an die im digitalen Speichermedium gespeicherte Computersoftware, wenn der digitale Code mit dem vorbestimmten Sicherheitscode übereinstimmt; und

(e) Zurückweisen des digitalen Speichermediums, wenn der digitale Code nicht mit dem vorbestimmten Sicherheitscode übereinstimmt.

10. Verfahren nach Anspruch 9, bei dem der Sicherheitscode über eine vorgegebene Anzahl von Bits verfügt, von denen jedes durch den ersten oder zweiten logischen Zustand repräsentiert ist.

11. Verfahren nach einem der Ansprüche 9 oder 10, ferner mit einem zusätzlichen Schritt des Anzeigens eines vorbestimmten Videobilds nur dann, wenn der Schritt des Vergleichens des digitalen Codes mit einem vorbestimmten Sicherheitscode ermittelt, dass der digitale Code mit dem vorbestimmten Sicherheitscode übereinstimmt.

12. Verfahren nach einem der Ansprüche 9 oder 10, ferner mit einem zusätzlichen Schritt des Betreibens des Systems gemäß im digitalen Speichermedium gespeicherter Software nur dann, wenn der Schritt des Vergleichens des digitalen Codes mit dem vorbestimmten Sicherheitscode ermittelt, dass der digitale Code mit dem vorbestimmten Sicherheitscode übereinstimmt.

13. Verfahren nach einem der Ansprüche 9 oder 10, ferner mit einem zusätzlichen Schritt des Ausführens einer zweiten Verifizierung, bei der das System einen weiteren, in einem dem System zugeordneten Speicher gespeicherten Code mit einem unter einer vorbestimmten Adresse im digitalen Speichermedium gespeicherten Code vergleicht, und einem Schritt des Zurückweisens des digitalen Speichermediums, wenn der weitere Code nicht mit dem unter der vorbestimmten Adresse im digitalen Speichermedium gespeicherten Code übereinstimmt.

14. Verfahren nach Anspruch 13, bei dem der weitere Code ein Markenlogo ist und das Verfahren den zusätzlichen Schritt des Anzeigens des Logos auf ei-

nem dem System zugeordneten Anzeigeschirm aufweist, wenn der weitere Code mit dem unter der vorbestimmten Adresse im digitalen Speichermedium gespeicherten Code übereinstimmt.

15. Vorrichtung zum Lesen eines in einem digitalen Speichermedium mit einer ersten und einer zweiten Seite und einer Anzahl von auf der ersten Seite des digitalen Speichermediums in Form einer Spur von Datenbits gespeicherten Datenbits, und mit einem in der Spur gespeicherten Sicherheitscode, der als Modulation eines Positionsversatzes des körperlichen Orts der Datenbits gegenüber einem Nenn-Spurort definiert ist, wobei die Vorrichtung Folgendes aufweist:

- eine Einrichtung zum Lesen der Modulation des körperlichen Versatzes gegenüber der Nenn-Spurposition einer Anzahl von auf dem digitalen Speichermedium gespeicherten Bits;

dadurch gekennzeichnet, dass die Vorrichtung ferner Folgendes aufweist:

- eine Detektoreinrichtung (3; 20) zum Erkennen eines als Binärmodulation des körperlichen Positionsversatzes definierten Codes, wobei ein Versatz der Datenbits als erster logischer Zustand definiert ist und fehlender Versatz gegenüber dem Nenn-Spurort als zweiter logischer Zustand definiert ist, wobei die Detektoreinrichtung über einen mit dem Ausgang der Leseeinrichtung verbundenen Eingang verfügt;
- eine Erkennungseinrichtung (22) zum Ermitteln; ob der von der Detektoreinrichtung (3; 20) erfasste Code mit einem in einem der Vorrichtung zugeordneten Speicher gespeicherten vorbestimmten Sicherheitscode übereinstimmt; und
- eine Steuerung (24) zum Steuern der Wiedergabe von auf dem digitalen Speichermedium gespeicherten Daten abhängig von einem Ausgangssignal der Erkennungseinrichtung (22).

16. Vorrichtung nach Anspruch 15, bei der der Sicherheitscode über eine vorgegebene Anzahl von Bits verfügt, von denen jedes durch den ersten oder zweiten logischen Zustand repräsentiert ist.

17. Vorrichtung nach einem der Ansprüche 15 oder 16, ferner mit:

- einer Einrichtung zum Lesen von an einer Anzahl von Datenbitorten unter einer vorbestimmten Adresse im digitalen Speichermedium gespeicherten Daten, wobei die Leseeinrichtung über einen Ausgang verfügt;
- einer Einrichtung zum Erfassen eines zweiten Codes, der in der Anzahl von Datenbitorten unter der vorbestimmten Adresse gespeichert ist, wobei die Erfassungseinrichtung mit dem Ausgang der Leseeinrichtung verbunden ist; und
- einer zweiten Erkennungseinrichtung zum Ermitteln, ob der zweite Code mit einem weiteren vorbestimmten Code übereinstimmt, der in einem der Vorrichtung zugeordneten Speicher gespeichert ist.

18. Vorrichtung nach Anspruch 17, bei der der zweite Code ein Logo definiert und die Vorrichtung ferner eine Einrichtung zum Anzeigen des Logos aufweist, wenn ermittelt wird, dass der zweite Code mit dem weiteren vorbestimmten Code übereinstimmt.

19. Verfahren zum Speichern eines Sicherheitscodes auf einem plattenförmigen digitalen Speichermedium, mit den folgenden Schritten:

(a) Erzeugen eines digitalen Sicherheitscodes;
(b) Bewegen des digitalen Speichermediums in Bezug auf eine Laserquelle (42);
(c) Positionieren der Laserquelle (42) über einem nicht bespielten Spurort des digitalen Speichermediums (45);

gekennzeichnet durch die folgenden Schritte:
(e) Aufzeichnen einer Anzahl digitaler Datenbits auf dem digitalen Speichermedium (45) durch Binärmodulation eines Positionsversatzes des Laserstrahls auf dem digitalen Speichermedium gegenüber einer Nenn-Spurposition zum Definieren eines logischen Zustands eines Datenbits des Sicherheitscodes, wobei ein Versatz der Datenbits gegenüber der Nenn-Spurposition als erster logischer Zustand definiert wird und fehlender Versatz gegenüber der Nenn-Spurposition als zweiter logischer Zustand definiert wird.

20. Verfahren nach Anspruch 19, bei dem der erste logische Zustand dem logischen Wert "1" entspricht.

21. Verfahren nach Anspruch 19, bei dem der Schritt des Versetzens des Laserstrahls gegenüber der Nenn-Spurposition für eine Positionsversatz-Wobbelung der Spurposition mit einer Wobbelungsfrequenz sorgt, die im Wesentlichen 22,05 kHz entspricht.

22. Verfahren nach einem der Ansprüche 19 bis 21, bei dem der Sicherheitscode über eine vorgegebene Anzahl von Bits verfügt, von denen jedes durch den ersten oder zweiten logischen Zustand repräsentiert ist.

23. Vorrichtung zum Ausführen des Verfahrens nach einem der Ansprüche 19 bis 22, **gekennzeichnet**

durch:

- einen Sicherheitscodegenerator (37) zum Liefern des digitalen Sicherheitscodes;
- wobei ein Ausgang des Sicherheitscodegenerators (37) mit einem Eingang eines akustooptischen Ablenkungsverstärkers (38) verbunden ist;
- wobei ein Ausgang des akustooptischen Ablenkungsverstärkers (38) mit einem ersten Eingang einer akustooptischen Ablenkungsschaltung (39) verbunden ist; und
- einen Aufzeichnungslaser (42) mit einem Ausgang, der mit einem zweiten Eingang der akustooptischen Ablenkungsschaltung (39) verbunden ist.

Revendications

1. Support (1) de mémorisation numérique, ayant une première face et une seconde face,

   plusieurs bits de données mémorisés sur une piste de la première face, et
   un code de sécurité mémorisé sur la piste, le code de sécurité étant défini comme une modulation d'un décalage de position de l'emplacement physique des bits de données par rapport à un emplacement nominal de piste,

   caractérisé en ce que
   la modulation du décalage de position de l'emplacement physique est une modulation binaire, telle qu'un décalage des bits de données est défini comme étant un premier état logique et une absence de décalage par rapport à l'emplacement nominal de piste est définie comme étant un second état logique.

2. Support de mémorisation numérique selon la revendication 1, dans lequel le décalage de position des bits de données a une fréquence de déviation de 22,05 kHz.

3. Support de mémorisation numérique selon la revendication 1, dans lequel la modulation du décalage de position de l'emplacement physique des bits de données s'effectue dans la direction radiale du support d'enregistrement.

4. Support de mémorisation numérique selon la revendication 1, dans lequel le premier état logique est un état logique "1".

5. Support de mémorisation numérique selon la revendication 1, dans lequel le code de sécurité est mémorisé à un format non-retour à zéro.

6. Support de mémorisation numérique selon la revendication 1, dans lequel le support de mémorisation numérique est un disque optique numérique compact, et le code de sécurité est mémorisé dans la zone de sa table des matières TOC.

7. Support de mémorisation numérique selon la revendication 6, dans lequel le code de sécurité est mémorisé de façon répétée dans la zone de la table des matières TOC du disque compact.

8. Support de mémorisation numérique selon l'une des revendications précédentes, dans lequel le code de sécurité a un nombre déterminé de bits, chacun étant représenté par l'un des premier et second états logiques.

9. Procédé destiné à empêcher un système fonctionnant avec un logiciel d'ordinateur de fonctionner avec un logiciel non autorisé contenu sur un support de mémorisation numérique ayant plusieurs bits de données mémorisés sur une face du support de mémorisation sous forme d'une piste de données numériques, selon lequel un code de sécurité est mémorisé sur la piste du support d'enregistrement, le code de sécurité étant défini par modulation par décalage de position de l'emplacement physique des bits de données par rapport à un emplacement nominal de piste,

   le procédé étant caractérisé en ce qu'il comprend les étapes suivantes :

   (a) l'examen d'une piste de bits de données sur le support de mémorisation numérique pour la détermination d'une modulation par décalage binaire des bits de données, un décalage des bits de données par rapport à l'emplacement nominal de pistes étant défini comme étant un premier état logique et une absence de décalage des bits de données par rapport à l'emplacement nominal de pistes étant définie comme un second état logique,
   (b) la démodulation de la modulation du décalage binaire pour la détermination d'un code numérique qui représente le code de sécurité,
   (c) la comparaison du code numérique avec un code prédéterminé de sécurité pour la détermination du fait que le code numérique démodulé correspond au code prédéterminé de sécurité,
   (d) l'acceptation du support de mémorisation comme étant authentique et le passage de la commande du système fonctionnant avec un logiciel au logiciel d'ordinateur mémorisé sur le support de mémori-

sation numérique, lorsque le code numérique correspond au code prédéterminé de sécurité, et

(e) le rejet du support de mémorisation numérique lorsque le code numérique ne correspond pas au code prédéterminé de sécurité.

10. Procédé selon la revendication 9, dans lequel le code de sécurité a un nombre prédéterminé de bits, chacun étant représenté par l'un des premier et second états logiques.

11. Procédé selon la revendication 9 ou 10, comprenant en outre une étape supplémentaire d'affichage d'une image vidéo prédéterminée uniquement lorsque l'étape de comparaison du code numérique avec un code prédéterminé de sécurité indique que le code numérique correspond au code prédéterminé de sécurité.

12. Procédé selon la revendication 9 ou 10, comprenant en outre une étape supplémentaire de mise en oeuvre du système à l'aide d'un logiciel mémorisé sur le support de mémorisation numérique seulement lorsque l'étape de comparaison du code numérique au code prédéterminé de sécurité indique que le code numérique correspond au code prédéterminé de sécurité.

13. Procédé selon la revendication 9 ou 10, comprenant en outre une étape supplémentaire d'exécution d'une seconde vérification dans laquelle le système compare un code supplémentaire mémorisé dans une mémoire associée au système à un code mémorisé à une adresse prédéterminée sur le support de mémorisation numérique, et une étape de rejet du support de mémorisation numérique lorsque le code supplémentaire ne correspond pas au code mémorisé à l'adresse prédéterminée sur le support de mémorisation numérique.

14. Procédé selon la revendication 13, dans lequel le code supplémentaire est un logo approprié et le procédé comprend l'étape supplémentaire d'affichage du logo sur un écran d'affichage associé au système lorsque le code supplémentaire correspond au code mémorisé à l'adresse prédéterminée sur le support de mémorisation numérique.

15. Appareil de lecture d'un code de sécurité conservé sur un support de mémorisation numérique ayant une première face et une seconde face et plusieurs bits de données mémorisés sur la première face du support de mémorisation numérique sous forme d'une piste de bits de données, et un code de sécurité mémorisé dans la piste, le code de sécurité étant défini comme étant une modulation par décalage de position de l'emplacement physique des bits de données par rapport à un emplacement nominal de piste, dans lequel l'appareil comprend :

un dispositif de lecture de la modulation par décalage physique par rapport à la position nominale de piste de plusieurs bits de données conservés sur le support de mémorisation numérique,

caractérisé en ce que l'appareil comporte en outre :

un dispositif détecteur (3 ; 20) destiné à détecter un code qui est défini comme une modulation binaire du décalage de position physique afin qu'un décalage des bits de données soit défini comme un premier état logique et une absence de décalage par rapport à l'emplacement nominal de piste soit définie comme un second état logique, le dispositif détecteur ayant une entrée connectée à la sortie du dispositif de lecture,

un dispositif discriminateur (22) destiné à déterminer si le code détecté par le dispositif détecteur (3 ; 20) correspond à un code prédéterminé de sécurité conservé dans une mémoire associée à l'appareil, et

un organe de commande (24) destiné à commander la reproduction des données conservées dans le support de mémorisation numérique en fonction d'un signal de sortie du dispositif discriminateur (22).

16. Appareil selon la revendication 15, dans lequel le code de sécurité a un nombre déterminé de bits, représentés chacun par l'un des premier et second états logiques.

17. Appareil selon la revendication 15 ou 16, comprenant en outre :

un dispositif de lecture de données conservées dans plusieurs emplacements de bits de données à une adresse prédéterminée sur le support de mémorisation numérique, le dispositif de lecture ayant une sortie,

un dispositif de détection d'un second code mémorisé à plusieurs emplacements de bits de données à l'adresse prédéterminée, le dispositif de détection étant connecté à la sortie du dispositif de lecture, et

un second dispositif discriminateur destiné à déterminer si le second code correspond à un code prédéterminé supplémentaire conservé dans une mémoire associée à l'appareil.

18. Appareil selon la revendication 17, dans lequel le second code détermine un logo, et dans lequel l'appareil comporte en outre un dispositif d'affichage du logo, lorsqu'il est déterminé que le second code cor-

respond au code prédéterminé supplémentaire.

19. Procédé de mémorisation d'un code de sécurité sur un support de mémorisation numérique en forme de disque, comprenant les étapes suivantes :

(a) la création d'un code numérique de sécurité,
(b) le déplacement du support numérique de mémorisation par rapport à une source laser (42),
(c) le positionnement de la source laser (42) au-dessus d'un emplacement de piste non enregistrée du support de mémorisation numérique (45),

caractérisé par les étapes suivantes :
(e) l'enregistrement de plusieurs bits de données numériques sur le support de mémorisation numérique (45) par modulation binaire d'un décalage de position du faisceau laser sur le support de mémorisation numérique par rapport à une position nominale de piste pour la détermination d'un état logique d'un bit de données du code de sécurité, dans lequel un décalage des bits de données par rapport à la position nominale de piste est défini comme étant un premier état logique et une absence de décalage par rapport à la position nominale de piste est définie comme étant un second état logique.

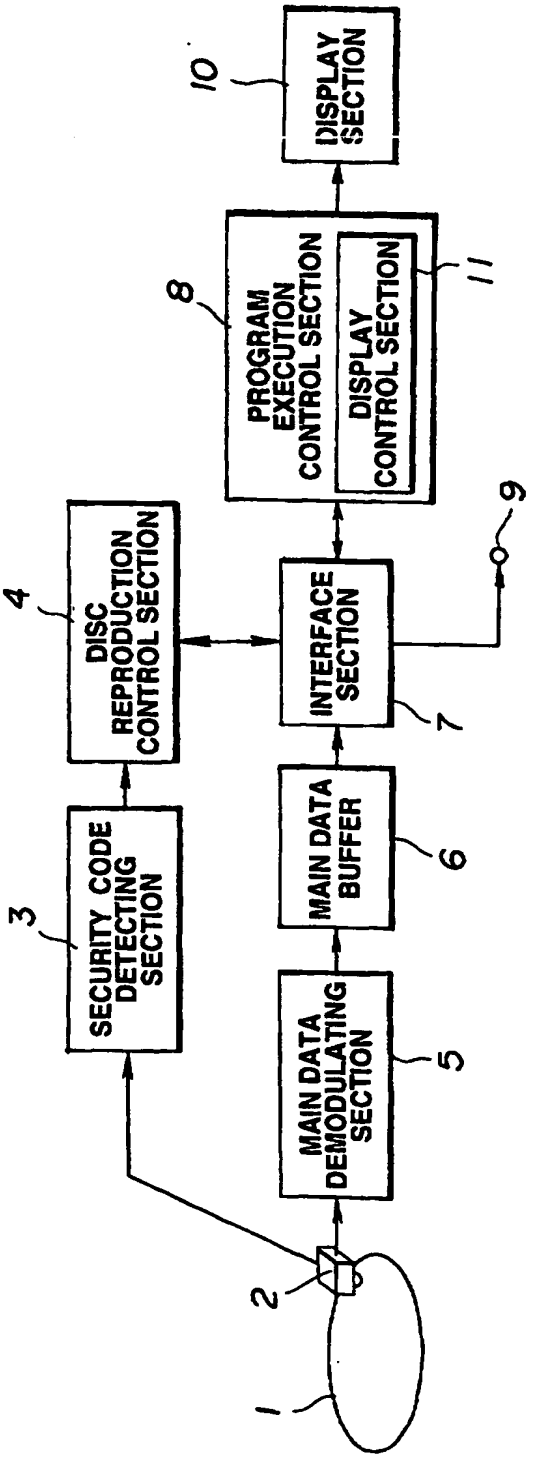
20. Procédé selon la revendication 19, dans lequel le premier état logique est un état logique "1".

21. Procédé selon la revendication 19, dans lequel l'étape de décalage du faisceau laser par rapport à la position nominale de piste donne une déviation de décalage de position de piste ayant une fréquence de déviation pratiquement égale à 22,05 kHz.

22. Procédé selon l'une des revendications 19 à 21, dans lequel le code de sécurité a un nombre déterminé de bits, chacun étant représenté par l'un des premier et second états logiques.

23. Appareil pour la mise en oeuvre du procédé selon l'une des revendications 19 à 22, caractérisé en ce que l'appareil comporte :

un générateur (37) de code de sécurité destiné à donner le code numérique de sécurité,
une sortie du générateur (37) de code de sécurité étant connectée à une entrée d'un amplificateur (38) de déflexion acoustique optique,
une sortie de l'amplificateur de déflexion acoustique optique (38) étant connectée à une première entrée d'un circuit (39) de déflexion acoustique optique, et
un laser d'enregistrement (42) ayant une sortie connectée à une seconde entrée du circuit (39) de déflexion acoustique optique.



ESSENTIAL PART OF
DISC REPRODUCING APPARATUS

FIG.1

FIG.2A

FIG.2B

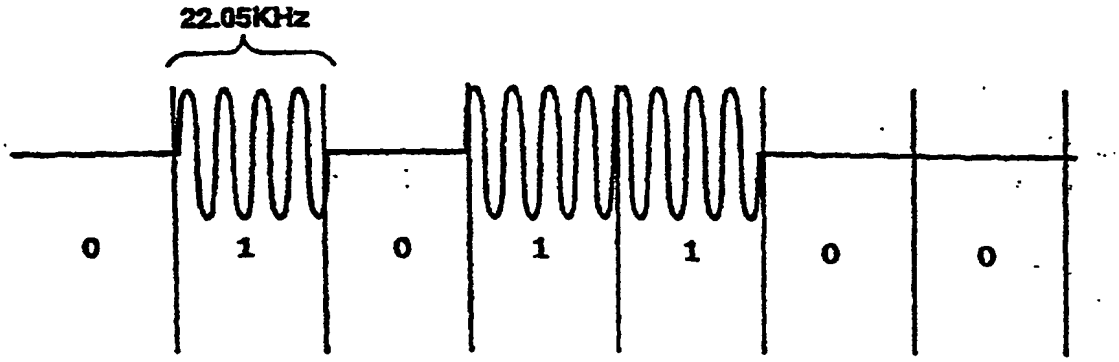


FIG.3

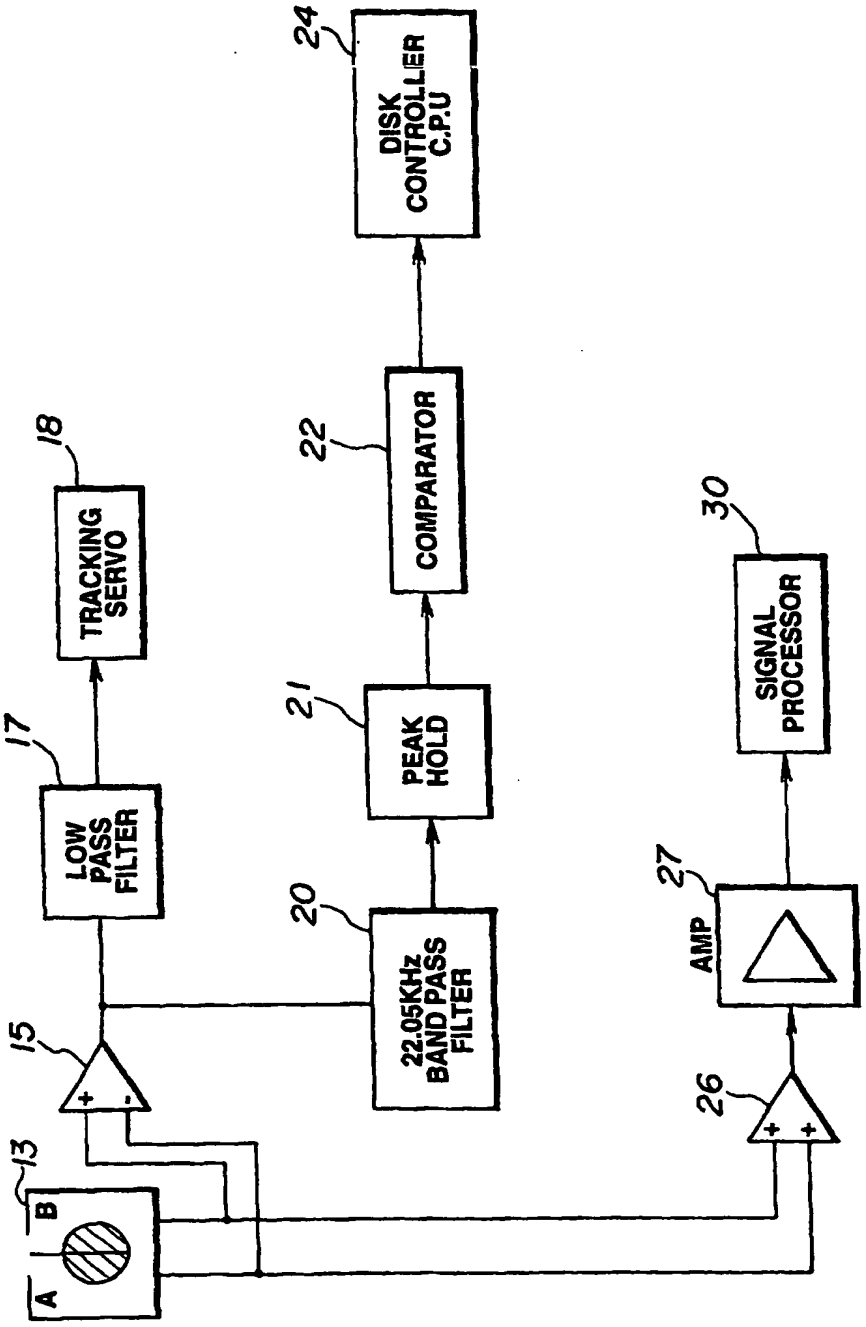
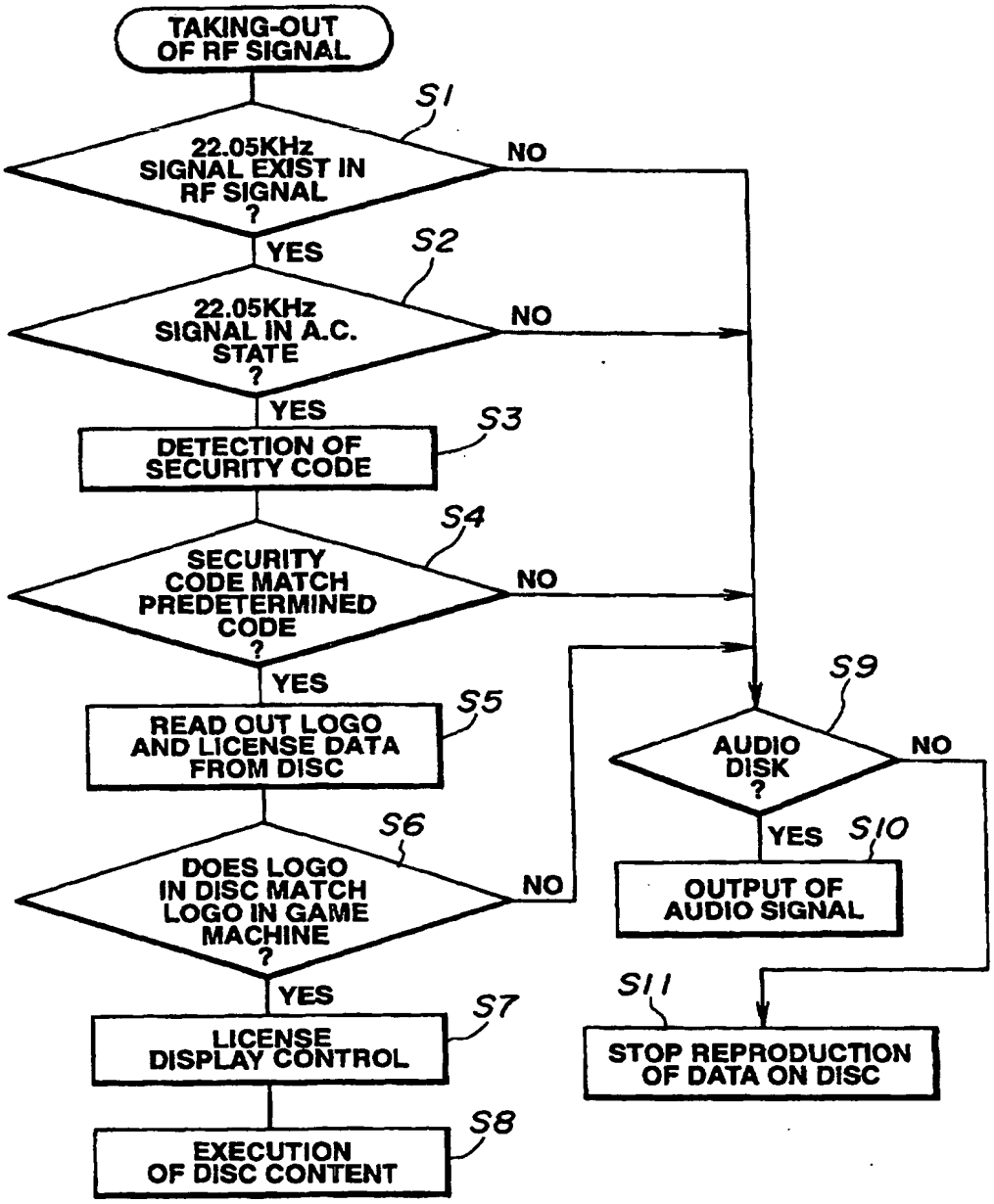
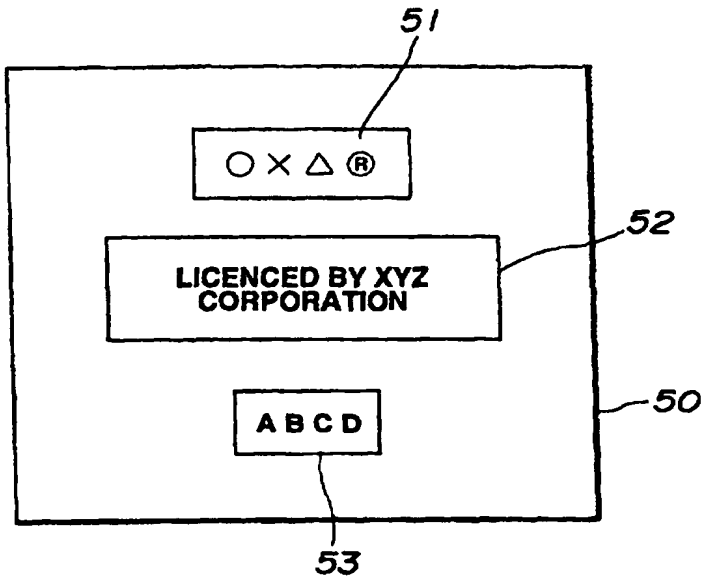

24
DISK CONTROLLER C.P.U
22
COMPARATOR
18
TRACKING SERVO
21
PEAK HOLD
30
SIGNAL PROCESSOR
17
LOW PASS FILTER
20
22.05KHz BAND PASS FILTER
27
AMP
15
26
13
B
A

FIG.4



FLOW DIAGRAM OF SYSTEM OPERATION

FIG.5



EXAMPLE OF DISPLAY PICTURE

FIG.6

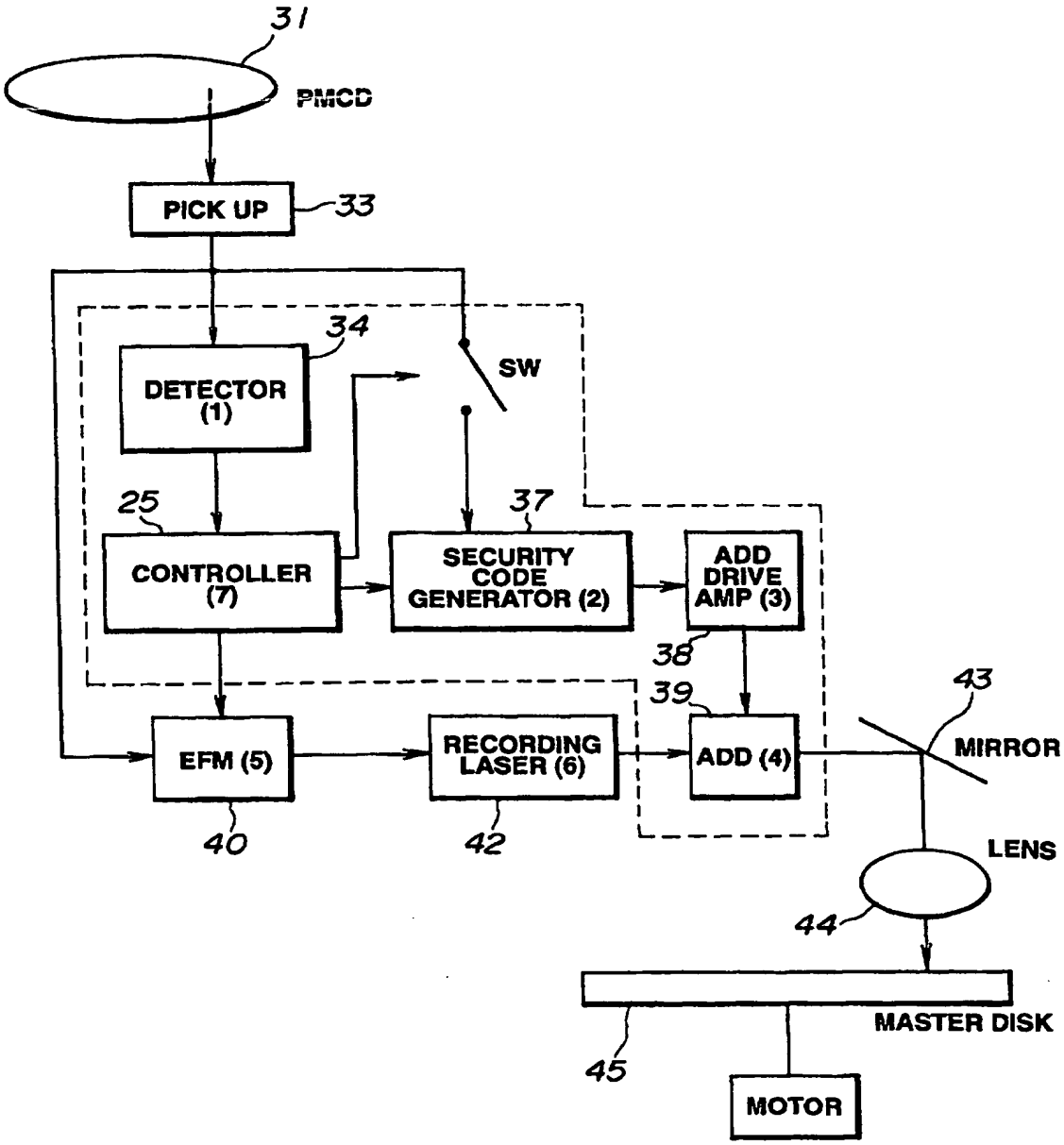

31
PMCD
PICK UP
33
34
DETECTOR (1)
SW
25
37
CONTROLLER (7)
SECURITY CODE GENERATOR (2)
ADD DRIVE AMP (3)
38
39
43
MIRROR
EFM (5)
RECORDING LASER (6)
ADD (4)
40
42
LENS
44
MASTER DISK
45
MOTOR

FIG.7